What is claimed is:

1. A method for auditing an organization's internal controls for handling information technology (IT) configurations and vulnerabilities comprising:

creating a technology summary summarizing relevant IT systems;

determining IT systems to test;

identifying gaps in internal controls used to identify and remedy at least one of vulnerabilities and improper configuration standards;

performing at least one of reviewing and testing existing internal controls; and

generating comments based on results of said at least one of reviewing and testing.

2. The method of claim 1, wherein the step of performing comprises:

evaluating control standards for relevant IT systems;

compiling an organization's assertions regarding internal controls over a vulnerability management process;

obtaining the organization's documentation concerning internal controls over the vulnerability management process;

documenting gaps in the organization's internal controls over the vulnerability management process;

communicating said documented gaps to the organization;

testing relevant IT systems for vulnerability exposure; and

reaching a conclusion on the organization's ability to achieve said organization's assertions regarding internal controls over the vulnerability management process.

3. The method of claim 2, wherein Advisor is used to evaluate control standards for relevant IT systems and to test relevant systems for vulnerability exposure.

4. A method for evaluating internal controls governing the management of IT configurations and vulnerabilities comprising:

defining the internal controls;

organizing a project team to conduct an evaluation;

documenting and evaluating the internal controls at an entry level;

documenting and evaluating the internal controls at a process, a transaction and an application level; and

evaluating overall effectiveness, identifying matters for improvement and establishing a monitoring systems.

5. A system for auditing an organization's internal controls for handling information technology (IT) configurations and vulnerabilities comprising:

a creating unit for creating a technology summary summarizing relevant IT systems;

a determining unit for determining IT systems to test;

an identifying unit for identifying gaps in internal controls used to identify and remedy at least one of vulnerabilities and improper configuration standards;

a performing unit for performing at least one of reviewing and testing existing internal controls; and

a generating unit for generating comments based on results of said at least one of reviewing and testing.

6. The system of claim 5, wherein the performing unit additionally:

evaluates control standards for relevant IT systems;

compiles an organization's assertions regarding internal controls over a vulnerability management process;

obtains the organization's documentation concerning internal controls over the vulnerability management process;

documents gaps in the organization's internal controls over the vulnerability management process;

communicates said documented gaps to the organization;

testes relevant IT systems for vulnerability exposure; and

reaches a conclusion on the organization's ability to achieve said organization's assertions regarding internal controls over the vulnerability management process.

7. The system of claim 6, wherein Advisor is used to evaluate control standards for relevant IT systems and to test relevant systems for vulnerability exposure.

8. A system for evaluating internal controls governing the management of IT configurations and vulnerabilities comprising:

a defining unit for defining the internal controls;

an organizing unit for organizing a project team to conduct an evaluation;

an entry-level-documenting unit for documenting and evaluating the internal controls at an entry level;

an application-level-documenting unit for documenting and evaluating the internal controls at a process, a transaction and an application level; and

an evaluating unit for evaluating overall effectiveness, identifying matters for improvement and establishing a monitoring systems.

9. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for auditing an organization's internal controls for handling information technology configurations and vulnerabilities comprising:

creating a technology summary summarizing relevant IT systems;

determining IT systems to test;

identifying gaps in internal controls used to identify and remedy at least one of vulnerabilities and improper configuration standards;

performing at least one of reviewing and testing existing internal controls; and

generating comments based on results of said at least one of reviewing and testing.

10. The computer system of claim 9, wherein the step of performing comprises:

evaluating control standards for relevant IT systems;

compiling an organization's assertions regarding internal controls over a vulnerability management process;

obtaining the organization's documentation concerning internal controls over the vulnerability management process;

documenting gaps in the organization's internal controls over the vulnerability management process;

communicating said documented gaps to the organization;

testing relevant IT systems for vulnerability exposure; and

reaching a conclusion on the organization's ability to achieve said organization's assertions regarding internal controls over the vulnerability management process.

11. The computer system of claim 10, wherein Advisor is used to evaluate control standards for relevant IT systems and to test relevant systems for vulnerability exposure.

12. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for auditing an organization's internal controls for handling information technology configurations and vulnerabilities comprising:

defining the internal controls;

organizing a project team to conduct an evaluation;

documenting and evaluating the internal controls at an entry level;

documenting and evaluating the internal controls at a process, a transaction and an application level; and

evaluating overall effectiveness, identifying matters for improvement and establishing a monitoring systems.